

**A BAYESIAN APPROACH TO RELIABILITY AND CONFIDENCE**

**Final Report**

**NASA/ASEE Summer Faculty Fellowship Program 1989**

**Johnson Space Center**

<b>Prepared By:</b>	<b>Ron Barnes, Ph.D.</b>
<b>Academic Rank:</b>	<b>Associate Professor</b>
<b>University &amp; Department:</b>	<b>University of Houston- Downtown Department of Applied Mathematical Sciences One Main Street Houston, Texas 77002</b>
<b>NASA/JSC Directorate:</b>	<b>Safety, Reliability, and Quality Assurance</b>
<b>Division:</b>	<b>Reliability and Maintainability</b>
<b>JSC Colleague:</b>	<b>Richard Heydorn</b>
<b>Date Submitted:</b>	<b>August 4, 1989</b>
<b>Contract Number:</b>	<b>NGT 44-001-800</b>

## ABSTRACT

In response to the Challenger accident, NASA has expanded its risk assessment studies from a completely qualitative Failure Modes and Effects Analysis/Critical Items Lists (FMEA/CIL) to include some quantitative investigations like Probability Risk Assessment (PRA).

Dr. Richard Heydorn (Reliability) presented lectures on quantitative methods to the Vehicle Reliability Branch at the request of branch chief, Malcolm Himel. As an outgrowth, the Extended Duration Orbiter - Weakest Link study is being developed. Three avionics subsystems and one with mechanical components, the freon coolant loop, have been identified as posing potential problems to keeping the Orbiter in space for long periods of time. The intent of the study is to devise a standard methodology for constructing system reliability diagrams and identifying what data is needed and/or potentially available. The data will then be utilized in Bayesian probability models to estimate reliabilities and consequently identify any significant problem subsystems.

Classical statistical methods are not suitable for many NASA problems. At NASA, data records are often sparse, incomplete or in a form not amenable to classical confidence estimates. Also, since problem-identification-problem-correction is employed throughout the operating lifetime of many NASA systems, the usefulness of failure history data is greatly compromised. Bayesian analysis addresses such concerns since it allows for the insertion of informed opinions instead of/or in addition to observational data on failures.

Our summer work generalized some of Dr. Heydorn's results for systems with a constant failure rate (exponential model) that is generally applicable to avionic systems, to the case of a variable failure rate (Weibull model) which contains the exponential as a special case. The Weibull model applies to reliability systems with burn in and/or wear out stages including most mechanical systems.

In the exponential case a closed form was obtained for the Bayesian estimate of the reliability function of a single component. The reliability of a system can then be evaluated using the rules of probability. With these estimators it is also possible to calculate the probability that the true reliability of a component lies within a certain interval and estimate the probability that the reliability of a system lies in a certain interval.

Using Bayesian ideas it now becomes possible to handle situations which the classical analysis could not, namely: (1) how to handle problems where no failure data has been observed over a period of time and (2) how to incorporate expert opinions into the probability calculations along with the data on failures.

In the more general Weibull (variable failure rate) model we have obtained a Bayesian estimator for the reliability which reduces to a closed form for special cases. In these cases the rest of the Bayesian analysis can be pursued.

Further investigations will consider the numerical evaluation of the Weibull Bayesian estimator for reliability in the general case. Bayesian estimates for the reliability of single components and systems, and probability statements similar to those described for the exponential model may then be pursued. The results can then be applied to the freon coolant subsystem of the Extended Duration Orbiter - Weakest Link study.

## INTRODUCTION

In response to the Challenger accident and subsequent reports by governmental commissions [NRC, House Report] , NASA has expanded its risk assessment studies from a completely qualitative Failure Modes and Effects Analysis/Critical Items List (FMEA/CIL) to some quantitative investigations including Probability Risk Assessment (PRA).

FMEA/CIL is basically a bottom-up approach. Individual components of a system are analyzed. Their individual failure modes are determined and the effects of each type of failure are investigated. On the basis of this analysis, various critical categories are assigned to each failure mode of each component. One shortcoming of the FMEA/CIL approach is that it does not assign priorities. As Charles Harlan, director of the Safety, Reliability, and Quality Assurance Directorate at NASA/JSC has noted, "There are many criticality 1 items in a system like the Shuttle, or in your car for that matter, . . . How do you distinguish the very unlikely failure you can live with from the likely ones you have to fix?" He further stated that "Our present system doesn't assess priorities, and we're going to modify that. We need a relative ranking of the risk associated with each failure mode." [SPECTRUM]

Probability Risk Assessment addresses this shortcoming. In contradistinction to FMEA/CIL, PRA is a top-down method in which possible failure modes of the entire system are first identified. The possible ways this could occur are enumerated and for each fault, chains of faults are traced out until eventually one arrives at the failure of a single component or a human error. A downward branching fault tree is constructed in which probabilities are assigned to the basic faults and then the total probability of various failure paths can be computed. In this way their relative contributions to the total risk are assessed.

NASA's historical preference for a qualitative approach to reliability and shunning of quantitative procedures is documented in the June 1989 special issue on risk analysis in SPECTRUM. As noted by the SPECTRUM editors:

During the Apollo days NASA contracted with General Electric to do a PRA to determine the chances of landing a man on the moon and safely returning him to earth. When the study indicated the probability of success was less than five percent, NASA decided the study would do "irreparable harm..." and they "studiously stayed away from [numerical risk assessment] as a result.

Will Willoughby, NASA head of Reliability and Safety at the time, added:

"That's when we threw all that garbage out and got down to work... Statistics don't count for anything . They have no place in engineering anywhere." [SPECTRUM]

As a result, NASA adapted qualitative failure modes and effects analysis (FMEA).

The SPECTRUM article further pointed out that in the 1970's and early 1980's, because of political realities it became necessary for NASA to show that the Shuttle would be "cheap and routine, rather than expensive and risky." Such pressures led to examples where data was disregarded and arbitrary assignments of risk levels were made.

The deliberate decision by NASA to forgo quantitative (probabilistic) risk analyses determined the type of data NASA decided to collect. For example no elapsed times were originally recorded for components on the shuttle. The failure to record various kinds of data, which was recoverable, precluded many forms of statistical analyses from even being considered.

After the Challenger accident the National Research Council (NRC) and the House of Representative committee on Science and Technology issued reports, in addition to the Presidential Commission [Roger's Report]. The Congressional report noted that:

Without some means of estimating the probability of failure of the various elements, it is not clear how NASA can focus its attention and resources as effectively as possible on the most critical systems.

In a similar vein the NRC noted:

The Committee views the NASA/CIL waiver decision making process as being subjective with little in the way of formal and consistent criteria for approval or rejection of waivers. Waiver decisions appear to be driven almost exclusively by the design based FMEA/CIL retention rationale rather than being based on an integrated assessment of all inputs to risk management.

In response to the Challenger accident and these reports, NASA is now changing in favor of a "willingness to explore other things" [SPECTRUM]. NASA has contracted two PRA pilot projects and has developed workshops to train engineers and others in quantitative risk assessment techniques.

### **One Approach**

In this spirit, Dr. Richard Heydorn presented lectures on quantitative methods to the Vehicle Reliability Branch at the request of branch chief, Malcolm Himel. As an outgrowth, the Extended Duration Orbiter - Weakest Link study is being developed. Three avionics subsystems and one with mechanical components, the freon coolant loop, have been identified as posing potential problems to keeping the Orbiter in space for long periods of time. The intent of the study is to devise a standard methodology for constructing

system reliability diagrams and identifying what data is needed and/or potentially available. The data will then be utilized in Bayesian probability models to estimate reliabilities and consequently identify any significant problem subsystems.

Classical statistical methods are not suitable for many NASA problems. At NASA, data records are often sparse, incomplete or in a form not amenable to classical confidence estimates. Also, since problem-identification-problem-correction is employed throughout the operating lifetime of many NASA systems, the usefulness of failure history data is greatly compromised. Bayesian analysis addresses such concerns since it allows for the insertion of informed opinions instead of/or in addition to observational data on failures.

### **PRELIMINARY WORK ON A BAYESIAN APPROACH TO RELIABILITY AND CONFIDENCE**

Prior to my arrival to take part in the NASA Summer Faculty Fellow program, Dr. Heydorn had begun Bayesian investigations into reliability by modeling the reliability of a single component (e.g. valve, piston, computer chip, etc...) assuming a constant rate of failure. The reliability of a system of components can then be modeled using the laws of probability.

The Bayesian approach was selected because of the shortcomings of classical statistical analysis with NASA data as pointed out earlier. In particular, in cases with very few data values on failures, classical confidence intervals for the reliability may be larger than the unit interval  $[0,1]$  and hence quite meaningless. Similarly since classical estimates of reliability depend on the failure history sample, an extreme but not uncommon situation in which no failures are recorded can lead one to blindly believe that we can conclude a high confidence in high reliability. The Bayesian approach appears to be much more fruitful in that it can address such data difficulties.

In the case where the failure rate  $\lambda$  is constant, under the fairly general assumptions that (a) the number of failures in any two disjoint time intervals are independent and (b) the distribution of the number of failures in any time interval depends only on the interval length, it follows that for  $t > 0$ ,  $N(t)$  the number of failures from time 0 to  $t$  is a random variable defined on a probability space  $\Omega_\lambda$ .  $N(\omega, t)$  has a Poisson probability distribution with

$$\Pr(N(t) = n) = ((\lambda t)^n / n!) e^{-\lambda t} \quad (1)$$

For this process let  $x(\omega, t) = 1$  if  $N(\omega, t) = 0$  and let  $x(\omega, t) = 0$  if  $N(\omega, t) > 0$ . The reliability function is then defined as:

$$R(t) = \Pr(x(t) = 1) = P(N(t) = 0) = e^{-\lambda t} \quad (2)$$

Note that the reliability is just the probability that the component is still operating after time  $t$  (i.e. it has not failed on the interval  $(0, t]$ ). Note that in this case the reliability function is exponential.

Assuming that a component was observed (or tested) over a period of time length  $T$  and was seen to have failed  $n$  times, a logical question to ask is

"What is the probability that after some additional time interval of length  $t$ , the component will not have failed again?"

Since we know the component starts in an operating state and since the events  $\{x(t) = 1\}$  and  $\{N(t) = n\}$  occur in disjoint time intervals, the Poisson assumption (a) shows that

$$\Pr[x(t) = 1 | N(T) = n] = \Pr[x(t) = 1], \quad (3)$$

i.e. the failure history has no direct bearing on the reliability when we assume the component starts in an operating state.

Heydorn has pointed out the inadequacies of classical statistical analysis, as noted earlier in this paper. He has shown that the Bayesian estimator of the reliability, given that  $n$  failures were recorded in an earlier time interval of length  $T$ , and assuming a uniform prior distribution of  $\lambda$  on  $(0, \ell]$  and then letting  $\ell \rightarrow \infty$ , is given by:

$$E(R_{\lambda}(t) | N(T) = n) = P(x(t) = 1 | N(T) = n) = 1/(1 + t/T)^{n+1} \quad (4)$$

The expression

$$E(R_{\lambda}(t) | N(T) = n) = 1/(1 + t/T)^{n+1} \quad (5)$$

is the key to his discussion and allows him to make probability statements about the reliability of the component. Heydorn also has shown that the Bayesian estimator for the reliability given by expression (4) is a consistent estimator for the true reliability  $R(t)$ . Exploiting (5) Heydorn has obtained expressions for the probability that the reliability of a component (and of a system of components) lies in specified intervals of values between 0 and 1. He notes that this formulation addresses some of the data problems with classical statistical analysis. For example if no failures were recorded in time  $T$  (not an uncommon occurrence when testing highly reliable components) expression (5) gives

$$E(R_{\lambda}(t) | N(T) = 0) = 1/(1 + t/T) \quad (6)$$

and Heydorn is able to exploit this expression, while in the classical case no such expression is possible! Heydorn also indicates how the Bayesian approach can be used to incorporate expert opinion into the probabilistic process even when no historical data may be available. Essentially the uniform prior on  $(0, \infty)$  is in some sense the "least informative" prior since it assumes that every positive value of  $\lambda$  is equally likely of being the "true"

value of the constant rate  $\lambda$ . Given additional expert opinion, it is often possible to incorporate that opinion into the choice of an alternate prior distribution for  $\lambda$ . Heydorn illustrates this with an example and shows how a system containing a mixture of components, some with failure data and others with only expert opinions on the failure mechanisms, can be probabilistically analyzed.

## DISCUSSION

For these summer investigations, the first objective was to extend the results to the more general case where the failure rate (hazard function) is non-constant. A good model for a non-constant hazard function is the Weibull distribution,  $W(\lambda, \beta)$ , which can model both "break in" and "wear out" failure conditions in a system and contains the constant failure rate model as a special case. The discussion that follows considers the following formulation of the Weibull distribution.

$$\begin{aligned} f(t, \lambda, \beta) &= \lambda \beta t^{\beta-1} e^{-\lambda t^\beta} \\ R(t, \lambda, \beta) &= e^{-\lambda t^\beta} \quad \lambda, \beta, t > 0 \\ h(t, \lambda, \beta) &= \lambda \beta t^{\beta-1} \end{aligned} \quad (7)$$

Note that in the special case when  $\beta = 1$  the hazard function reduces to the constant  $\lambda$  and the reliability function is the exponential function, i.e. one has the constant failure rate model considered earlier.

In Weibull reliability analysis it is often the case that the value of the shape parameter  $\beta$  is known. In fact the literature sharply divides into the case where  $\beta$  is known and only the scale parameter  $\lambda$  is unknown and the more general case where both parameters are unknown. In the case where  $\beta$  is known considerable analysis has occurred [Martz].

If one assumes a non-constant intensity function  $h(t, \lambda, \beta) = \lambda \beta t^{\beta-1}$ , it is easy to show under assumptions similar to (a) and (b) given earlier that the probability of  $n$  failures occurring by time  $T$  is given by

$$P[N(T) = n] = (e^{-\lambda T^\beta} (\lambda T^\beta)^n) / n! \quad (8)$$

This is usually referred to as the nonhomogeneous Poisson process.

## SPECIAL CASE

Now for the Weibull model with  $\beta$  known, the Bayesian estimate for the reliability can be calculated (assuming  $\lambda$  has a uniform prior and the limiting process is carried out as before) and one sees that

$$E(R_\lambda(t) | N(T)=n) = P[x(t) = 1 | N(T)=n] = 1 / (1 + (t/T)^\beta)^{n+1} \quad (9)$$

In this special case the Bayesian estimate is seen to be a consistent estimator of the reliability function (7). With expression (8) one is able to make probability statements about the reliability of a component (and system) as Heydorn did for the exponential case for situations that classical reliability theory can not address. The inclusion of expert opinion into the process can also proceed as was indicated earlier.

### GENERAL CASE

In the more general case where both  $\beta$  and  $\lambda$  are unknown, we assume they are unknown values of random variables that must be estimated. We assume prior uniform distribution on  $(0, \ell_\lambda]$  and  $(0, \ell_\beta]$  and eventually take the limiting values so that  $\lambda$  and  $\beta$  may take on any nonnegative values. In a sense, these are the least informative priors since they assume that every possible value for  $\lambda$  (and  $\beta$ ) is equally likely of occurring i.e. we have no additional information on the true values of  $\lambda$  and  $\beta$ .

Preliminary investigations indicated that  $N(T)$ , the number of failures recorded in time  $T$ , is not sufficient to ensure that the corresponding Bayesian estimate of reliability is a consistent estimator of the true reliability.

It is well known [Bain, Finklestein, et al.] that if  $T_1, \dots, T_n$  denote the first  $n$  successive times of failure of a Weibull process ( $T_1 \leq T_2 \leq \dots \leq T_n$ ) then the likelihood function is given by:

$$f(t_1, \dots, t_n, \lambda, \beta) = \lambda^n \beta^n \left( \prod t_i \right)^{\beta-1} e^{-\lambda(t_n)^\beta} \quad (10)$$

The Bayesian Estimator of reliability in this case (for uniform priors on  $(0, \ell_\lambda]$   $(0, \ell_\beta]$  and taking limits) reduces to:

$$E[R_\lambda(t) \mid T_1 = t_1, \dots, T_n = t_n] = P[x(t) = 1 \mid T_1 = t_1, \dots, T_n = t_n] \\ = \frac{[\ln[t_n \prod (t_n/t_i)]]^{n+1}}{n!} \quad \text{limit}_{\ell \rightarrow \infty} \int_0^\ell \frac{\beta^n e^{-\beta \ln[t_n \prod (t_n/t_i)]} d\beta}{[1 + (t/t_n)^\beta]^{n+1}} \quad (11)$$

While expression (11) does not have a closed form in general, a few observations are in order:

(a) The form of (11) indicates that  $t_n$  and  $\prod t_i$  together carry all the information necessary to obtain the Bayesian estimate of reliability. We note that in the classical analysis  $t_n$  and  $\prod t_i$  are joint sufficient statistics [Bain].

(b) The Bayesian estimate (11) is a consistent estimator for  $R(t)$ , the true reliability. In fact, we conjecture that an even more general result holds.

Namely, under some rather general conditions we believe it is possible to show that for any estimator  $\Theta$  of  $\theta$ ,

$$E[\Theta \mid x_1, \dots, x_n] \rightarrow \theta \text{ (as } n \rightarrow \infty) \quad (12)$$

(c) In the special case that  $t = t_n$ , i.e. one wants to estimate the reliability after time  $t$  in the future that is equal to the total elapsed time for the first  $n$  past failures, expression (11) reduces to

$$E[R_\lambda(t) \mid T_1 = t_1, \dots, T_n = t_n] = (1/2)^{n+1} \quad (13)$$

With this closed form one can again make probability statements about the reliability of a component, conditioned on the failure times  $t_1, \dots, t_n$ . In particular the probability that this system has not failed after  $t$  units of time given that it failed  $n$  times over a period of time  $t$  in the past is  $(1/2)^{n+1}$ . For example if one had data on 1 failure after 10,000 hours of operation then the probability that the component (starting from an operating state) will not fail during the next 10,000 hours is  $(1/2)^2 = 1/4 = .25$ . Expression (13) suggests that if no failures were encountered in  $t$  units of time then the probability that there will be no failures in a future time interval of  $t$  units (starting from an operating state) would be  $1/2 = .50$ . In some sense there is a 50/50 chance of the component failing in the next  $t$  units of time if it has not failed in a prior  $t$  units of time.

Again with expression (13), using the laws of probability it is possible to obtain expressions for the probability that the reliability of a component (or a system of components) lies in a specified range of values between 0 and 1.

## CONCLUSION

This report outlined the historical evolution of NASA's interest in quantitative measures of reliability assessment. The introduction of some quantitative methodologies into the Vehicle Reliability Branch of the SR&QA Division at JSC was noted along with the development of the Extended Orbiter Duration - Weakest Link study which will utilize quantitative tools for a Bayesian statistical analysis.

Extending the earlier work of my NASA sponsor, Richard Heydorn, we have been able to produce a consistent Bayesian estimate for the reliability of a component and hence by a simple extension for a system of components in some cases where the rate of failure is not constant but varies over time. Mechanical systems in general have this property since the reliability usually decreases markedly as the parts degrade over time. While we have been able to reduce the Bayesian estimator to a simple closed form for a large class of such systems, the form for the most general case needs to be attacked by the computer. Once a table is generated for this form, we will have a numerical form for the general solution. With this, the corresponding probability statements about the reliability of a system can be made in the most general setting. Note that the utilization of uniform Bayesian priors represent a "worst case" scenario in the sense that as we incorporate more expert opinion into the model we will be able to improve the strength of the probability calculations.

## REFERENCES

1. National Research Council, Aeronautics and Space Engineering Board, Committee on Shuttle Criticality Review and Hazard Analysis audit, "Post-Challenger Evaluation of Space Shuttle Risk Assessment and Management," January 1988.
2. Committee on Science and Technology, U.S. House of Representatives, "Investigation of the Challenger Accident", Ninety - Ninth Congress, October 29, 1986.
3. Bell, Trudy E. and Karl Esch, "Special Report: the Space Shuttle: A Case of Subjective Engineering," IEEE SPECTRUM, 42-46, June 1989.
4. Presidential Commission on the Space Shuttle Challenger Accident, "Report to the President", June 6, 1986.
5. Heydorn, Richard, unpublished lecture notes on quantitative methods for reliability, NASA/JSC, Reliability and Maintainability Division, Spring 1989.
6. Martz, Harry F. and Ray A. Waller, Bayesian Reliability Analyses, John Wiley and Sons, New York, 1982.
7. Bain, Lee J. Statistical Analysis of Reliability and Life-Testing Models, Marcel Dekker Inc., New York, 1978.
8. Finkelstein, J. M., "Confidence Bands on the Parameters of the Weibull Process," Technometrics, Vol. 18, No. 1, 115-117, February 1976.

# APPENDIX

$$\begin{aligned}
 E[R_{\lambda}(t) \mid T_1 = t_1, \dots, T_n = t_n] &= P[x(t) = 1 \mid T_1 = t_1 \dots T_n = t_n] \\
 &= \frac{\lim_{\beta \rightarrow \infty} \frac{1}{\ell_{\beta}} \int_0^{\ell_{\beta}} \int_0^{\ell_{\lambda}} \beta^n \lambda^n (\prod t_i)^{\beta-1} e^{-\lambda(t_n)^{\beta}} e^{-\lambda t^{\beta}} d\lambda d\beta}{\lim_{\lambda \rightarrow \infty} \frac{1}{\ell_{\beta}} \frac{1}{\ell_{\lambda}} \int_0^{\ell_{\beta}} \int_0^{\ell_{\lambda}} \beta^n \lambda^n (\prod t_i)^{\beta-1} e^{-\lambda(t_n)^{\beta}} d\lambda d\beta}
 \end{aligned}$$

